

Date September 14, 2000

Sir:



09/19/00

Transmitted herewith for filing under 35 U.S.C. 111 and 37. C.F.R. 1.53 is the patent application of:

INVENTOR(S): JOHN EVERSON, and JAMES W. NORRIS

FOR: AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES

Enclosed are:

- ☒ Certificate of Mailing with Express Mail Mailing Label No. EL618532394US
- ☒ 1 sheets of drawing(s)
- ☒ Combined Declaration and Power of Attorney
- ☒ An Assignment of the invention to SPRINT SPECTRUM, L.P. together with the recording fee of \$40.00.
- ☐ A verified statement to establish small entity status under 37 CFR 1.9 and 37 CFR 1.27.
- ☐ Information Disclosure Statement

The filing fee has been calculated as shown below:

	(Col. 1)	(Col. 2)
FOR:	NO. FILED	NO. EXTRA
BASIC FEE		
TOTAL CLAIMS	12-20=	* 0
INDEP. CLAIMS	2-3=	* 0
MULTIPLE DEPENDENT CLAIM PRESENT		

* If the difference in col. 1 is less than zero, enter "0" in Col. 2

SMALL ENTITY		OR	OTHER THAN A SMALL ENTITY	
RATE	FEE		RATE	FEE
	\$ 345.00	OR		\$ 890.00
x 9		OR	x 18	
x 39		OR	x 78	
+130		OR	+260	
TOTAL	\$	OR	TOTAL	\$690.00

Please charge my Deposit Account No. 19-0522 in the amount of \$. A duplicate of this sheet is enclosed.

- ☒ A check in the amount of \$690.00 to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 19-0522. A duplicate of this sheet is enclosed.
- ☒ Any additional filing fees required under 37 CFR 1.16.
- ☒ Any patent application processing fees under 37 CFR 1.17.
- ☒ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 19-0522. A duplicate copy of this sheet is enclosed.
- ☒ Any patent application processing fees under 37 CFR 1.16.
- ☐ The issue fee set in 37 CFR 1.18 at or before the mailing of the Notice of Allowance, pursuant to 37 CFR 1.311(f).
- ☒ Any fees under 37 CFR 1.16 for presentation of extra claims.

By

Thomas B. Luebbert, Reg. No. 37,874



23589

09/19/00
JC820 U.S. PTO

CERTIFICATION UNDER 37 C.F.R. 1.10

Enclosed for filing is the application for United States Letters Patent of JOHN EVERSON and JAMES W. NORRIS, Attorney Docket No. 30604, entitled AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES, including: **Transmittal, Specification, Claims, Abstract, 1 sheet informal drawings, Combined Declaration and Power of Attorney, \$690.00 filing fee, Assignment Cover Sheet, Assignment, \$40.00 recordation fee, and return card.**

EL618532394US
"Express Mail" mailing number

September 19, 2000
Date of Deposit

I hereby certify that the above-noted papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to BOX NEW APPLICATION, Assistant Commissioner for Patents, Washington, DC 20231.

Heidi Caragan
Name of person mailing

Heidi Caragan
Signature of person mailing

AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER
PROFILING USING DYNAMIC DIRECTORY SERVICES

5

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention relates to the fields of computer authentication, application authorization and user profiling. More particularly, the invention relates to the use of dynamic directory services (DDS) to dynamically store information in a directory server that can be used for authentication, application authorization, and user profiling purposes to eliminate the need for numerous authorization and access control schemes with a single standard directory based set of applications.

15

2. DESCRIPTION OF THE PRIOR ART

Many computer networks require users to be authenticated before they are allowed access thereto. Similarly, many computer applications and/or programs can only be accessed or used by authorized users. Computer users are typically authenticated and/or authorized by access control and security programs that contain or consult user profiles or databases (data repositories) containing access control information for the users. These access control and security programs typically require the entry of user IDs, passwords, etc., before users are allowed access to the networks and/or programs and applications.

25

Most networks, programs, and applications that have secured entries have their own proprietary access control and security systems (front and back). This requires computer users who wish to gain access to more than one network, application, and/or program during a computer session to repeatedly re-enter their user IDs, passwords, etc., each time they attempt to transfer from one network to another or from one application or program to another. This also requires each network, application, and program to have and maintain its own separate access control information for all users.

30

SUMMARY OF THE INVENTION

The present invention solves the above-described problems and provides a distinct advance in the art of computer authentication and authorization. More

particularly, the present invention provides a system and method for authenticating and authorizing computer users with a single, standard, directory-based set of applications.

The present invention combines Dynamic Directory Services (DDS) with a directory access protocol such as the Lightweight Directory Access Protocol (LDAP) to provide authentication and authorization for secured networks, applications, and programs. The present invention uses DDS to store dynamic information such as session information or user ID information in a directory each time a user logs into the system and then maintains the information in the directory until the user logs out. While the information exists in the directory, it can be queried by any other program, application, or network that uses LDAP or other directory protocol to authenticate or authorize the user for the network or application. The present invention therefore eliminates the need to maintain separate access control systems for each secured network, program, or application.

The method and system of the present invention may also be used to provide a more convenient on-line shopping cart and for user profiling and session profiling purposes.

These and other important aspects of the present invention are described more fully in the detailed description below.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

A preferred embodiment of the present invention is described in detail below with reference to the attached drawing figure, wherein:

Fig. 1 is a schematic diagram of computer and communications equipment that may be used to implement certain aspects of a preferred embodiment of the present invention.

The drawing figure does not limit the present invention to the specific embodiments disclosed and described herein. The drawing Figure is not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention combines a directory access protocol such as the Lightweight Directory Access Protocol (LDAP) or X.500 with Dynamic Directory Services

(DDS) to provide authentication and application-authorization for secured networks, applications, and programs. Instead of using a directory for static information such as user names, addresses, and phone numbers, however, the present invention uses a directory to store dynamic information such as session information or a shopping cart.

- 5 When a user logs into the system of the present invention, a user object is created in a directory and remains in the directory until the user logs out of the system. Then, any other applications and/or networks accessed by the computer user during the session may simply query the directory to obtain authorization and authentication information. A simple query to the directory can also indicate how many users are logged into the
- 10 system at any given moment.

- The present invention can be implemented in hardware, software, firmware, or a combination thereof. However, the invention is preferably implemented in software that operates computer and communication equipment such as the equipment identified by the numeral 10 in Fig. 1. The computer and communications
- 15 equipment broadly includes a plurality of user computers 12, one or more application servers 14, one or more authorization servers 16, one or more user profile databases 18, a directory 20, and a communications network 22. The computer equipment and software illustrated and described herein are merely examples of hardware and software that may be used to implement a preferred embodiment of the present invention and
- 20 may be replaced with other computer equipment and software without departing from the scope of the present invention.

- The user computers 12 are entirely conventional and may be, for example, personal computers or even internet appliances. The user computers are each preferably equipped with a web browser and an internet connection such as a modem,
- 25 an ISDN or DSL converter, or a cable modem so that they can access web sites on the Internet in a conventional manner.

- The application servers 14 are coupled with the user computers 12 via the communications network 22 and are provided for running applications on behalf of the user computers. The application servers may be any computing devices such as
- 30 network or server computers. The application servers may be used to handle all application operations between the browser-based computers 12 and a company's back end business applications or databases. Because many databases cannot interpret

commands written in HTML, the application servers may serve as translators, allowing computer users to search for information with a browser.

The authorization servers 16 are coupled with the user computers 12 and the application servers 14 via the communications network 22 and are provided for authenticating and authorizing the user computers. The authorization servers may be any computing devices such as network or server computers running Windows NT, Novell Netware, Unix, or any other network operating system. As described in more detail below, the authorization servers may use any means for authenticating and authorizing users such as tokens, certificates, IDs, passwords, and access control measures.

The user profile databases 18 are coupled with the authorization servers 16 via the communications network 22 and are operable for storing certain profile information relating to the users of the user computers 12. The user profile databases may store, for example, user IDs, passwords, access control information such as what applications each computer user is allowed to access, shipping addresses, credit card numbers, information about previous purchases, and any other information useful for authentication, application authorization and user profiling and session profiling/management issues.

The directory 20 is coupled with the authorization servers 16 and the user profile databases 18 via the communications network 22 and is provided for storing directory information used in the present invention as described in more detail below. The directory may reside on any conventional computing device such as one or more network computers or server computers.

The communications network 22 may be a local area network, a wide area network, an intranet, an extranet, the Internet, or any other conventional network or combination of networks. In preferred forms, the user computers 12 may access the authorization servers 16 via the Internet, and the other components of the system 10 communicate via a local or wide area network.

The present invention is fully scalable in that any number of the above described devices of the system 10 can be added as needed. Moreover, none of the devices need to be from a particular vendor, or run on a particular platform. For example, there may be five different authorization servers 16 that perform authentication

and authorization of users, but each server may use a different method to authenticate users.

Operation of the computer and communications equipment 10 is controlled by one or more computer programs. Each computer program preferably comprises an ordered listing of executable instructions for implementing logical functions in the authorization servers 16 and the other computing devices as described herein. The computer programs can be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that can fetch the instructions from the instruction execution system, apparatus, or device, and execute the instructions. In the context of this application, a "computer-readable medium" can be any means that can contain, store, communicate, propagate or transport the program for use by or in connection with the instruction execution system, apparatus, or device.

The computer-readable medium can be, for example, but not limited to, an electronic, magnetic, optical, electro-magnetic, infrared, or semi-conductor system, apparatus, device, or propagation medium. More specific, although not inclusive, examples of the computer-readable medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable, programmable, read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disk read-only memory (CDROM). The computer-readable medium could even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

The following is a description of the operation of a preferred implementation of the present invention. In some alternative implementations, the functions described below in a particular order may occur out of the order described. For example, two steps described separately may in fact be executed substantially concurrently, or may sometimes be executed in the reverse order depending upon the functionality involved.

A user first launches some application or program in a conventional manner with one of the user computers 12. The particular application or program that

is launched is not important to the present invention and may include, for example, an internet browser, a Java application, a Java applet, a visual basic application, or any other program or application.

The application is initially directed to one of the authorization servers 16.

- 5 Which authorization server that is accessed may be based on any criteria including, but not limited to, the first authorization server that answers, a round-robin selection process, geographical criteria, or requirements based on the software or application being used.

- 10 The user next logs into the selected authorization server 16 using account or ID information that was established during a user-enrollment/setup process that occurred sometime in the past. The type of account information and authentication or authorization may be specific to the type of applications or network that the user has access to or the role that the user has been assigned.

- 15 In accordance with one important aspect of the present invention, the authorization server 16 creates a Session ID for the user after log-in. The Session ID may relate to the date or time that the user logged in, the media access control address of the user's computer 12, the TCP/IP address of the user's computer, the user's name, an account code for the user, a combination of any of these criteria, or any other criteria. It is important only that the Session ID be unique to the user and the particular
20 authorization server 16 that was accessed.

- The authorization server 16 then copies or links the Session ID or some derivative thereof to something on the user's computer 12 such as a cookie, shared application memory, or the computer's network address. It is important only that other applications launched by the user from the user computer be able to read or otherwise
25 determine this Session ID by accessing something on the user's computer.

- The authorization server 16 also creates an object representing the user or the Session ID and stores it in the directory 20 after log-in. The object name is preferably the same as the Session ID but may be any name relating to the Session ID. After the object is created and stored in the directory, the authorization server copies or
30 parses information about the user from the user profile database 18 and writes this information to the new directory object. The type of information depends on who the user is, what applications the user is allowed to use, what the role of the user is, and how the user was authenticated. The information could even include user IDs and

passwords for other applications to provide single log-in or sign-on capabilities. The information may also be encrypted, signed, or otherwise protected for security purposes.

After the user has successfully logged in, the menu or interface of the application the user attempted to launch is loaded so that the user may use the
5 launched application. This function may be performed by the authorization server 16, one of the application servers 14, or any other piece of computer equipment.

The above steps provide a means to authenticate and/or authorize the user for other applications and/or networks. Specifically, when the user attempts to access other applications and/or networks while he or she is still logged into the system,
10 these other applications may reference the Session ID on the user's computer. Using the Session ID, the other applications may read the user information that has been copied to the user's object in the directory for authentication and authorization purposes related to the new applications. The new applications may also be able to modify the information in the object so that the object could pass information to other applications
15 such as in a shopping cart environment described below.

The present invention may be used to replace numerous authorization and access control schemes with one standard, directory-based set of applications. The present invention allows all applications, computer programs, and networks that use a directory access protocol such as LDAP to access all user profile and access control
20 information created for a user while the user is logged into the system. This eliminates the need to create and maintain numerous authorization and access control schemes and requires a user to be authorized only once during a computer session.

The following is a more detailed example of how the above process may be implemented. Assume that the system 10 includes five authorization servers 16 and
25 that a user logs into authorization server number 2 (AS2) with a browser. AS2 first creates a unique, random Session ID for the user such as 82012053249. The authorization server then creates a cookie named "SID" in the user's browser and assigns it a value of AS2.82012053249.

The authorization server 16 also creates an object in the directory 20 and
30 relates it to the Session ID. The object is then populated with information from the user's profile, such as the user's ID, password, e-mail address, account number, etc.

The user is then offered a menu of applications/services that he or she is authorized to use or access. The user may select one of the applications or services,

for example a "View Bill" application. The View Bill application accesses the cookie named "SID" on the user's computer 12 and reads the value AS2.82012053249 from the cookie. The application then searches the directory 20 for the object associated with the cookie under the branch of the directory containing information for authorization server

5 AS2. The application reads the associated attributes (i.e. the account number, user ID, password) from the directory to determine what information the user is authorized to access. The View Bill application may then collect authorized information such as billing information from one of the application servers 14 and present it to the user on the screen of the user's computer.

10 When the user logs off, the object for the user stored in the directory 20 is deleted. The object may be deleted immediately after log-off or after a certain amount of time has elapsed. If the user attempts to log-in after the object has been deleted, the above process may be repeated for the same or even a different authorization server.

Another possible application of the present invention is for on-line

15 shopping carts. Assume, for example, that a user has already logged into the system 10 and that an object for the user has been created in the directory 20. Associated with the user's object is a shopping cart. The user browses shopping selections available via one or more merchandise servers and can add things to and or remove things from the shopping cart. If the user selects a book, for example, and indicates that he or she

20 wants to purchase the book, the ISBN number of the book is added to the user's object in the directory. As the user purchases more items, these items are also added to the user's object in the directory.

When the user is ready to purchase the items, a check-out server queries the object in the directory 20 and obtains information for all of the items selected by the

25 user. The check-out server may be a different server located in a different part of the network or may be connected with the other components in the network. The user information in the object may also contain credit card information so that purchases can be expedited. When the user logs out of the system 10, the user's object in the directory is preferably deleted to make room for objects for other users.

30 The present invention may also be used to determine how many users are logged into the system 10 at any given moment. Because a user object is created and maintained in the directory 20 whenever a user is logged into the system, a simple query to the directory can indicate how many users are currently logged into the system. For

example, the number of objects created under the AS2 branch of the directory indicates how many sessions were established by that particular authorization server. This information can be used to determine which authorization servers are over or under utilized.

5 Although the invention has been described with reference to the preferred embodiment illustrated in the attached drawing figures, it is noted that equivalents may be employed and substitutions made herein without departing from the scope of the invention as recited in the claims.

10 Having thus described the preferred embodiment of the invention, what is claimed as new and desired to be protected by Letters Patent includes the following:

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2

CLAIMS:

the steps of:

- a. storing security information for a plurality of computer users in a user profile database;
- b. receiving at an authorization server coupled with the user profile database log-in information from a computer user who has launched a computer application;
- c. in response to step b, creating a Session ID for the computer user with the authorization server;
- d. storing at least a portion of the Session ID on the user's computer;
- e. also in response to step b, creating an object associated with the computer user or the Session ID;
- f. storing the object in a directory coupled with the authorization server;
- g. copying at least some of the security information relating to the computer user from the user profile database to the object in the directory;
- h. comparing the log-in information entered by the computer user to the security information for the computer user and allowing the computer user access to the launched computer application if the user is an authenticated or authorized user of the computer application; and
- i. permitting other computer applications launched by the computer user to reference the Session ID on the user's computer so that the other computer applications may access the object for the computer user on the directory to authenticate or authorize the user for the other computer applications without requiring the user to re-enter the log-in information.

2. The method as set forth in claim 1, the security information including authentication and authorization information.

3. The method as set forth in claim 2, the authentication and authorization information including at least one of the following: user names, user IDs, passwords, public-key data, certificates, and access control information.

5 4. The method as set forth in claim 1, the Session ID being based on at least one of the following: a date on which the computer user launched the computer application; a time in which the computer user launched the computer application; a TCP/IP address of the computer user; a user name of the computer user; and an account code.

10

5. The method as set forth in claim 1, further including the steps of creating a shopping cart and storing the shopping cart along with the object in the directory.

15

6. The method as set forth in claim 5, further including the steps of allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart.

7. A system for authenticating and authorizing computer users, the system comprising:

a user profile database for storing security information for a plurality of computer users;

an authorization server coupled with the user profile database for receiving log-in information from a computer user who has launched a computer application, for creating a Session ID for the computer user, for storing at least a portion of the Session ID on the user's computer and for creating an object associated with the computer user or the Session ID; and

a directory coupled with the authorization server for storing the object created by the authorization server; and

the authorization server being further operable for copying at least some of the security information relating to the computer user from the user profile database to the object in the directory, comparing log information entered by the computer user to the security information for the computer user and allowing the computer user access to the launched computer application if the user is an authenticated or authorized user of the computer application, permitting other computer applications launched by the computer user to reference the Session ID on the user's computer so that the other computer applications may access the object for the computer user on the directory to authenticate or authorize the user for the other computer applications without requiring the user to re-enter the log-in information.

8. The system as set forth in claim 7, the security information including authentication and authorization information.

9. The system as set forth in claim 8, the authentication and authorization information including at least one of the following: user names, user IDs, passwords, public-key data, certificates, and access control information.

10. The system as set forth in claim 7, the Session ID being based on at least one of the following: a date on which the computer user launched the computer application; a time in which the computer user launched the computer application; a TCP/IP address of the computer user; a user name of the computer user; and an account code.

11. The system as set forth in claim 7, the authorization server being further operable for creating a shopping cart and storing the shopping cart along with the object in the directory.

12. The system as set forth in claim 11, the authorization server being further operable for allowing the user to select items to be purchased and storing information relating to the selected items in the shopping cart.

ABSTRACT OF THE DISCLOSURE

A system and method for authenticating and authorizing computer users with a single, standard, directory-based set of applications. The invention combines dynamic directory services (DDS) with a directory access protocol such as the light weight directory access protocol (LDAP) to provide authentication and application-authorization for secured networks, applications, and programs. Dynamic information such as session information or user ID numbers is stored in a directory each time a user logs into the systems and is maintained in the directory until the user logs out. While the information exists in the directory, it can be queried by other programs, applications, or networks that use a directory service to authenticate or authorize the user for the program, application, or network.

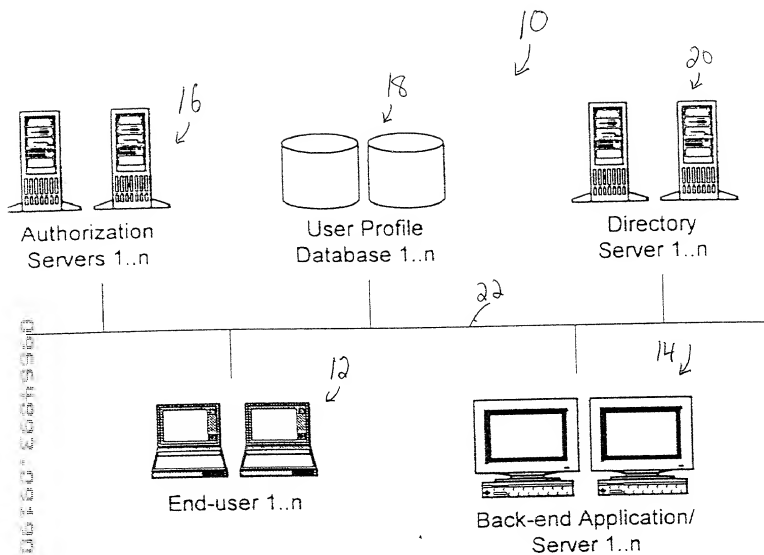


Fig. 1

COMBINED DECLARATION AND POWER OF ATTORNEY

(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is of the following type:

(check one applicable item below)

- ☒ original.
☐ design.
☐ supplemental.

NOTE: *If the declaration is for an International Application being filed as a divisional, continuation or continuation-in-part application, do not check next item; check appropriate one of last three items.*

- ☐ national stage of PCT.

NOTE: *If one of the following 3 items apply, then complete and also attach ADDED PAGES FOR DIVISIONAL, CONTINUATION OR C-I-P.*

NOTE: *See 37 C.F.R. § 1.63(d) (continued prosecution application) for use of a prior nonprovisional application declaration in the continuation or divisional application being filed on behalf of the same or fewer of the inventors named in the prior application.*

- ☐ divisional.
☐ continuation.

NOTE: *Where an application discloses and claims subject matter not disclosed in the prior application, or a continuation or divisional application names an inventor not named in the prior application, a continuation-in-part application must be filed under 37 C.F.R. § 1.53(b) (application filing requirements-nonprovisional application).*

- ☐ continuation-in-part (C-I-P).

INVENTORSHIP IDENTIFICATION

WARNING: *If the inventors are each not the inventors of all the claims, an explanation of the facts, including the ownership of all the claims at the time the last claimed invention was made, should be submitted.*

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am the original, first and sole inventor (*if only one name is listed below*) or an original, first and joint inventor

(if plural names are listed below) of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

AUTHENTICATION, APPLICATION-AUTHORIZATION, AND USER PROFILING USING DYNAMIC DIRECTORY SERVICES

SPECIFICATION IDENTIFICATION

The specification of which:

(complete (a), (b), or (c))

(a) ☒ is attached hereto.

NOTE: "The following combinations of information supplied in an oath or declaration filed on the application filing date with a specification are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 C.F.R. § 1.63:

"(1) name of inventor(s), and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration on filing;

"(2) name of inventor(s), and attorney docket number which was on the specification as filed; or

"(3) name of inventor(s), and title which was on the specification as filed."

Notice of July 13, 1995 (1177 O.G. 60).

(b) ☐ was filed on _____, as ☐ Application No. 0 / _____ or
☐ _____ and was amended on _____ (if applicable).

NOTE: Amendments filed after the original papers are deposited with the PTO that contain new matter are not accorded a filing date by being referred to in the declaration. Accordingly, the amendments involved are those filed with the application papers or, in the case of a supplemental declaration, are those amendments claiming matter not encompassed in the original statement of invention or claims. See 37 C.F.R. § 1.67.

NOTE: "The following combinations of information supplied in an oath or declaration filed after the filing date are acceptable as minimums for identifying a specification and compliance with any one of the items below will be accepted as complying with the identification requirement of 37 C.F.R. § 1.63:

"(1) name of inventor(s), and application number (consisting of the series code and the serial number; e.g., 08/123,456);

"(2) name of inventor(s), serial number and filing date;

"(3) name of inventor(s) and attorney docket number which was on the specification as filed;

"(4) name of inventor(s), title which was on the specification as filed and filing date;

"(5) name of inventor(s), title which was on the specification as filed and reference to an attached specification which is both attached to the oath or declaration at the time of execution and submitted with the oath or declaration; or

"(6) name of inventor(s), title which was on the specification as filed and accompanied by a cover letter accurately identifying the application for which it was intended by either the application number (consisting of the series code and the serial number; e.g., 08/123,456), or serial number and filing date. Absent any statement(s) to the contrary, it will be presumed that the application filed in the PTO is the application which the inventor(s) executed by signing the oath or declaration."

Notice of July 13, 1995 (1177 O.G. 60), M.P.E.P. § 601(a), 6th ed., rev.3.

- (c) ☐ was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____ (if any).

SUPPLEMENTAL DECLARATION (37 C.F.R. § 1.67(b))

(complete the following where a supplemental declaration is being submitted)

☐ I hereby declare that the subject matter of the

☐ attached amendment

☐ amendment filed on _____.

was part of my/our invention and was invented before the filing date of the original application, above identified, for such invention.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, § 1.56,

(also check the following items, if desired)

☐ and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent, and

☐ in compliance with this duty, there is attached an information disclosure statement, in accordance with 37 C.F.R. § 1.98.

PRIORITY CLAIM (35 U.S.C. § 119(a)-(d))

NOTE: "The claim to priority need be in no special form and may be made by the attorney or agent if the foreign application is referred to in the oath or declaration as required by § 1.63. The claim for priority and the certified copy of the foreign application specified in 35 U.S.C. § 119(b) must be filed in the case of an interference (§ 1.630), when necessary to overcome the date of a reference relied upon by the examiner, when specifically required by the examiner, and in all other situations, before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by a petition requesting entry and by the fee set forth in § 1.17(i). If the certified copy is not in the English language, a translation need not be filed except in the case of interference; or when necessary to overcome the date of a reference relied upon by the examiner; or when specifically required by the examiner, in which event an English language translation must be filed together with a statement that the translation of the certified copy is accurate." 37 C.F.R. § 1.55(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

(complete (d) or (e))

- (d) ☒ no such applications have been filed.
(e) ☐ such applications have been filed as follows.

NOTE: Where item (c) is entered above and the International Application which designated the U.S. itself claimed priority check item (e), enter the details below and make the priority claim.

**PRIOR FOREIGN/PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119(a)-(d)**

COUNTRY (OR INDICATE IF PCT)	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 USC 119
			<input type="checkbox"/> YES <input type="checkbox"/> NO
			<input type="checkbox"/> YES <input type="checkbox"/> NO
			<input type="checkbox"/> YES <input type="checkbox"/> NO
			<input type="checkbox"/> YES <input type="checkbox"/> NO
			<input type="checkbox"/> YES <input type="checkbox"/> NO

CLAIM FOR BENEFIT OF PRIOR U.S. PROVISIONAL APPLICATION(S)
(35 U.S.C. § 119(e))

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

PROVISIONAL APPLICATION NUMBER

FILING DATE

CLAIM FOR BENEFIT OF EARLIER U.S./PCT APPLICATION(S)
UNDER 35 U.S.C. § 120

[] The claim for the benefit of any such applications are set forth in the attached ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR CONTINUATION-IN-PART (C-I-P) APPLICATION.

ALL FOREIGN APPLICATION(S), IF ANY, FILED MORE THAN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS U.S. APPLICATION

NOTE: If the application filed more than 12 months from the filing date of this application is a PCT filing forming the basis for this application entering the United States as (1) the national stage, or (2) a continuation, divisional, or continuation-in-part, then also complete ADDED PAGES TO COMBINED DECLARATION AND POWER OF ATTORNEY FOR DIVISIONAL, CONTINUATION OR C-I-P APPLICATION for benefit of the prior U.S. or PCT application(s) under 35 U.S.C. § 120.

POWER OF ATTORNEY

I hereby appoint the following practitioner(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Robert D. Hovey	19,223	Andrew G. Colombo	40,565
Warren N. Williams	19,156	Scott R. Brown	40,535
Stephen D. Timmons	26,513	Tracy L. Bornman	42,347
John M. Collins	26,262	Tracey S. Truitt	43,205
Thomas H. Van Hoozer	32,761	Harley R. Ball	31,733
Thomas B. Luebbering	37,874	Steven J. Funk	35,875

(Check the following item, if applicable)

- ☐ I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.
- ☐ Attached, as part of this declaration and power of attorney, is the authorization of the above-named practitioner(s) to accept and follow instructions from my representative(s).

SEND CORRESPONDENCE TO
THOMAS B. LUEBBERING

DIRECT TELEPHONE CALLS TO:
(Name and telephone number)

☒ Address

THOMAS B. LUEBBERING
(816)474-9050

Attn: THOMAS B. LUEBBERING
HOVEY, WILLIAMS, TIMMONS & COLLINS
2405 Grand Boulevard, Suite 400
Kansas City, MO 64108-2519

☐ Customer Number _____

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

NOTE: Carefully indicate the family (or last) name, as it should appear on the filing receipt and all other document

NOTE: Each inventor must be identified by full name, including the family name, and at least one given name without abbreviation together with any other given name or initial, and by his/her residence, post office address and country of citizenship. 37 C.F.R. § 1.63(a)(3).

NOTE: Inventors may execute separate declarations/oaths provided each declaration/oath sets forth all the inventors. Section 1.63(a)(3) requires that a declaration/oath, inter alia, identify each inventor and prohibits the execution of separate declarations/oaths which each sets forth only the name of the executing inventor. 62 Fed. Reg. 53,131, 53,142, October 10, 1997.

Full name of sole or first inventor

John

(Given Name)

MICHAEL
(Middle Initial or Name)

Everson

Family (Or Last Name)

Inventor's signature

Date

9-12-00

Country of Citizenship

United States of America

Residence

11720 Troost Avenue, Kansas City, MO 64131

Post Office Address

11720 Troost Avenue, Kansas City, MO 64131

Full name of second joint inventor, if any

James

(Given Name)

W.
(Middle Initial or Name)

Norris

Family (Or Last Name)

Inventor's signature

Date

9-12-00

Country of Citizenship

United States of America

Residence

9935 North Harrison, Kansas City, MO 64155

Post Office Address

9935 North Harrison, Kansas City, MO 64155

Full name of third joint inventor, if any

(Given Name)

(Middle Initial or Name)

Family (Or Last Name)

Inventor's signature

Date

Country of Citizenship

Residence

Post Office Address

(check proper box(es) for any of the following added page(s)
that form a part of this declaration)

☐ **Signature** for fourth and subsequent joint inventors. *Number of pages added* _____

* * *

☐ **Signature** by administrator(trix), executor(trix) or legal representative for deceased or incapacitated inventor. *Number of pages added* _____

* * *

☐ **Signature** for inventor who refuses to sign or cannot be reached by person authorized under 37 C.F.R. § 1.47. *Number of pages added* _____

* * *

☐ Added page for **signature** by one joint inventor on behalf of deceased inventor(s) where legal representative cannot be appointed in time. (37 C.F.R. § 1.47)

* * *

☐ Added pages to combined declaration and power of attorney for divisional, continuation, or continuation-in-part (C-I-P) application.

☐ Number of pages added _____

* * *

☐ Authorization of practitioner(s) to accept and follow instructions from representative.

(If no further pages form a part of this Declaration,
then end this Declaration with this page and check the following item)

☒ This declaration ends with this page.